# ROLES & RESPONSIBILITIES

## PRIVACY ACT (PA) SYSTEMS OF RECORDS MANAGERS

# THE PRIVACY ACT OF 1974

… IS A RECORDS MANAGEMENT STATUTE

* how and why we collect information

* how we maintain information

* who has access

* how long we will maintain

# THE PRIVACY ACT REQUIRES THAT:

NOTICE BE GIVEN TO AN INDIVIDUAL WHENEVER PERSONALLY IDENTIFYING INFORMATION (PII) IS SOLICITED DIRECTLY FROM THAT INDIVIDUAL (PRIVACY ACT STATEMENT)

# THE PRIVACY ACT REQUIRES THAT:

PUBLICATION BE MADE IN THE FEDERAL REGISTER FOR:

- any new PA System of Records collection (PA System of Records Notice)

- any existing PA Systems of Records collection where the data collection, purpose, authority, disposition, etc. has changed

- any proposed computer matching program

# THE PRIVACY ACT REQUIRES THAT:

INFORMATION MAINTAINED IN PRIVACY ACT SYSTEM OF RECORDS FILE IS

- ACCURATE

- RELEVANT

- COMPLETE

- CURRENT

# THE PRIVACY ACT REQUIRES THAT:

INDIVIDUALS ARE ALLOWED ACCESS TO RECORDS ABOUT THEMSELVES

- when maintained in a NONEXEMPT PA System of Records file.

# THE PRIVACY ACT REQUIRES THAT:

"OFFICIAL" REQUESTS FOR NONCONSENSUAL DISCLOSURE OF INFORMATION BE PROCESSED IAW PROVISIONS ESTABLISHED BY THE PRIVACY ACT [5 U.S.C. §§ 552a(b)(1) through (b)(12)].

(b)(1) – For Official Use Only (within DoD)
(b)(2) – Required to be released by FOIA
(b)(3) – For pre-established official use (outside DoD)
(b)(4) – To Census Bureau (for census or survey)
(b)(5) – For statistical research
(b)(6) – To the National Archives
(b)(7) – For federal, state, and/or local civil or criminal law enforcement proceeding
(b)(8) – When health or safety of an individual is at issue
(b)(9) – For "official business" of Congress
(b)(10) – To GAO
(b)(11) – Pursuant to a court order
(b)(12) – To a consumer reporting agency under the Debt Collection Act (31 U.S.C. 3711(e).

# THE PRIVACY ACT REQUIRES THAT:

INDIVIDUALS BE ALLOWED TO FIND OUT ABOUT ANY UNAUTHORIZED SHARING OR DISCLOSURE OF INFORMATION MAINTAINED IN THEIR RECORDS (DISCLOSURE ACCOUNTING RECORDS).

Note: Exceptions to disclosure accounting requirements:

- disclosure made pursuant to Exception (b)(1) (FOUO)
- disclosure made pursuant to Exception (b)(2) (FOIA)
- disclosure made pursuant to Exception (b)(7) (but only during the specific time that the civil or criminal law enforcement proceeding is ongoing)

# THE PRIVACY ACT REQUIRES THAT:

INDIVIDUALS BE AFFORDED AN OPPORTUNITY AND MEANS BY WHICH TO CORRECT ANY INACCURACIES EXISTING IN THEIR RECORDS.

# THE PRIVACY ACT PROVIDES -

U.S. citizens and lawful aliens with guaranteed rights -

- To access/amend their records

- To appeal agency decisions regarding access or amendment

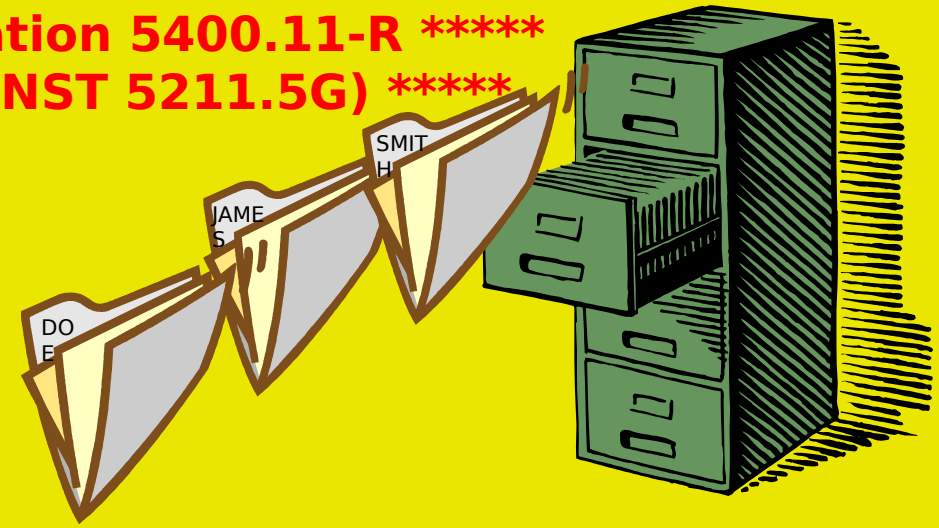
- To sue agencies for breaches/compromises

# PA SYSTEM OF RECORDS MANAGER RESPONSIBILITIES

## WHO IS A PRIVACY ACT SYSTEM OF RECORDS MANAGER?

**Any official responsible for the maintenance of a collection of records whereby records are routinely retrieved by someone's name or other similar personal identifier?**

******* See DoD Regulation 5400.11-R *******
******* (DON - SECNAVINST 5211.5G) *******



# PA SYSTEM OF RECORDS MANAGER RESPONSIBILITIES

- **Ensure that staff personnel receive annual Privacy Act training.**
- **Ensure that no data collection is undertaken unless there is a Federal Register published PA System of Records Notice that allows for the data collection.**
- **Ensure that data access is limited only to those personnel who have a specific "need to know" – not necessarily to all office personnel!**
- **Ensure that personal data is transmitted in a secure manner.**
- **Ensure that personal data is properly safeguarded during and after duty hours.**
- **Ensure that personal data is properly disposed of (rendered unrecognizable and beyond reconstruction).**
- **Ensure that staff personnel comply with the Privacy Act, DoD Privacy rules (DoD 5400.11-R), and the DON Privacy Act Fair Information Principles.**

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

## (1) IS YOUR STAFF PRIVACY TRAINED?

- CHECK TO SEE IF YOUR AGENCY HAS DEVELOPED PRIVACY TRAINING

  * DON has posted training at www.privacy.navy.mil/training

-ENSURE THAT YOUR STAFF COMPLETES PRIVACY TRAINING ANNUALLY

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

## (2) ARE YOUR DATA COLLECTIONS PROPERLY CONDUCTED?

* Ensure your staff consults with your command Privacy Office before:

- Initiating new data collections.

- Adding new elements to an existing, approved database.

- Creating or revising forms that collect personal data.

- Deploying surveys.

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

* Ensure your staff consults with your command Privacy Office before:

- Initiating new data collections.

- Adding new elements to an existing, approved database.

- Creating or revising forms that collect personal data.

- Deploying surveys.

* Ensure your staff includes a Privacy Act Statement on all forms, surveys, or websites that collect personal data.

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

## (3) IS YOUR STAFF SAFEGUARDING THE INFORMATION MAINTAINED IN YOUR FILES?

* Mark records "For Official Use Only – Privacy Sensitive" when created.

* For e-records, include "For Official Use Only – Privacy Sensitive" on data screens and in headers/footers of printouts.

* Place records in file cabinets, overhead bins, or desk drawers for overnight storage.

* Cover paper records when a third party enters your workspace.

* Use filter screens on terminals to blacken angular views.

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

## (4) IS YOUR STAFF FOLLOWING THE PRIVACY ACT FAIR INFORMATION PRINCIPLES?

* Periodically ask your staff to review the Code of Fair Information Principles (available at www.privacy.navy.mil).

* Ask your staff to immediately report to you, the Command Privacy Office, of the Command Information Technology staff all instances of personal data being openly posted (no permission levels) to a public or shared website, e-workplace, shared calendar, or shared drive.

# PA MANAGER'S ROADMAP FOR MEETING PRIVACY RESPONSIBILITIES

## (5) ARE YOU KEEPING PRIVACY AT THE TOP OF YOUR STAFF'S MINDS?

* Use staff meetings to stress good Privacy practices.

* Voice your commitment to protecting individual privacy.

* Applaud workers who practice good privacy principles!

* Remind staff to use caution when posting data to shared drives, e-work-places, or multi-access calendars.

* Question workers who leave personal data in the open.

# If You Have Access to Personal Data . . .

- **PKI Encrypt, UserID restrict, and/or password protect personal data placed on shared drives or the Intranet.**
- **Monitor your actions: If I do this, will I increase the risk of unauthorized access?**
- **Limit non-consensual access to those individuals who have an official need to know inside the agency and ensure that any non-consensual disclosures going outside the agency are permissible under Section (b) of the Privacy Act [5 U.S.C. 552a(b)(1) through (b)(12).**
- **It is your RESPONSIBILITY to protect personal information at all times.**

**Remember:**
**You may be subject to civil and criminal penalties for violating the Privacy Act.**

# Civil Penalties for Noncompliance with the Privacy Act

**The Privacy Act also imposes civil penalties on violators who:**

* Unlawfully refuse to amend a record
* Unlawfully refuse to grant access to records
* Fail to maintain accurate, relevant, timely and complete data
* Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.

**Penalties include:**

* Payment of actual damages
* Payment of reasonable attorney's fees
* Removal from employment

# Criminal Penalties for Noncompliance with the Privacy Act

- For knowingly and willfully disclosing Privacy Act data to any person not entitled to access:
  - Misdemeanor criminal charge, and a fine of up to $5000.
- For maintaining a System of Records without meeting the public notice requirements:
  - Misdemeanor criminal charge, and a fine of up to $5000.
- For knowingly and willfully requesting or obtaining records under false pretenses:
  - Misdemeanor criminal charge, and a fine of up to $5000.